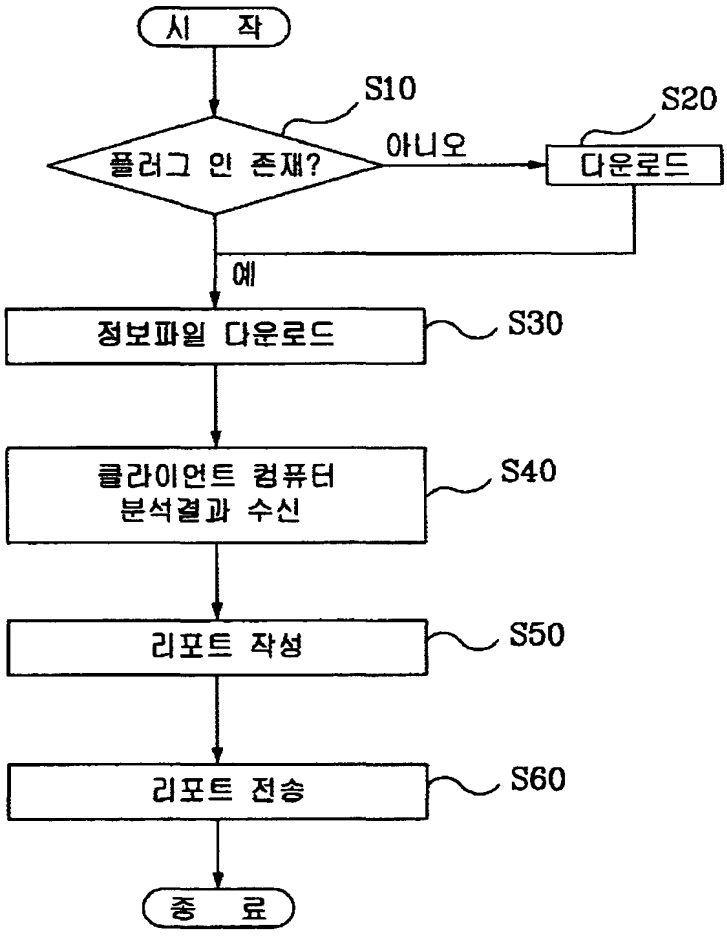
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020020022314 (43) Publication.Date. 20020327
(21) Application No.1020000055030 (22) Application Date. 20000919
(51) IPC Code:
G06F 15/16

(71) Applicant:
AHNLAB, INC.
(72) Inventor:
CHOI, BEOM GWON
(30) Priority:

(54) Title of Invention
METHOD AND SYSTEM FOR ANALYZING CLIENT COMPUTER

Representative drawing



(57) Abstract:

PURPOSE: A method and a system for analyzing a client computer are provided to confirm the exposure of a client computer to virus, to check a weak part of the client computer, and to solve related problems.

CONSTITUTION: The method comprises steps of offering an application program for analyzing a client computer system to a client computer through a communication network, receiving a result of analysis through the communication network(S40), writing a report based on the result(S50), and offering the report to the client computer (S60). The application program comprises an updating module to download the data files included in an application program, a version management module to maintain the data files in the newest version, an analysis item updating

module, a system analyzing module to analyze the system of a client computer, a result transfer module to transfer the result obtained by the system analyzing module, and a report output module to store the report as a file and output the report.

if display of image is failed, press (F5)

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[7]
G06F 15/16

(45) 공고일자 2003년04월14일
(11) 등록번호 10-0379915
(24) 등록일자 2003년03월31일

(21) 출원번호 10-2000-0055030
(22) 출원일자 2000년09월19일
(65) 공개번호 특2002-0022314
(43) 공개일자 2002년03월27일

(73) 특허권자 주식회사 안철수연구소
서울특별시 강남구 수서동 724 브이밸리 8층
(72) 발명자 최범권
경기도성남시수정구상적동294번지
(74) 대리인 특허법인 신성

심사관 : 마정윤

(54) 클라이언트 컴퓨터 분석 방법 및 그 시스템

요약

통신 네트워크 상에서 클라이언트 컴퓨터를 분석하기 위한 방법 및 그 시스템이 개시되어 있다. 본 발명은 클라이언트의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 클라이언트로 제공하는 제1단계, 어플리케이션 프로그램에 의한 클라이언트의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 제2단계, 시스템 분석 결과를 기초로 리포트를 작성하는 제3단계 및 작성된 리포트를 상기 통신 네트워크를 통해 클라이언트로 전송하는 제4단계를 포함하여, 종래의 패키지 형태의 프로그램이 아닌 온라인 프로그램으로서 인터넷이 가능한 곳에서는 별도의 복잡한 설치과정 없이 사용할 수 있으므로 프로그램을 휴대하고 다니거나 단일 컴퓨터에서만 사용하던 종래의 불편함을 해소하고, 어느 곳에서 컴퓨터를 사용하게 되더라도 위험성을 먼저 확인한 후에 사용할 수 있어 사전에 바이러스에 대한 위험을 제거하여 최근 급증하고 있는 바이러스에 대한 국가적인 차원의 손실을 예방할 수 있다.

대표도

도3

명세서

도면의 간단한 설명

도1은 본 발명에 따른 서버에서의 작업진행을 도시한 순서도,

도2는 본 발명에 따라 클라이언트 컴퓨터에서의 작업진행 과정을 도시한 순서도,

도3은 본 발명에 따른 서버와 클라이언트 컴퓨터의 구성도이다.

(도면의 주요 부분에 대한 부호의 설명>

100 : 서버
110 : HTTP 데몬
120 : 최신버전모듈
130 : 데이터베이스
140 : 공통 경로 인터페이스(CGI, Common Gateway Interface) 모듈
141 : 수신모듈
143 : 리포트 작성모듈
145 : 리포트 전송모듈
200 : 클라이언트 컴퓨터
210 : 웹브라우저
220 : 업데이트모듈
230 : 버전관리모듈
240 : 분석항목 업데이트모듈
250 : 시스템 분석모듈
260 : 분석결과 전송모듈
270 : 리포트 수신모듈
280 : 저장 및 경로재지정 모듈

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 통신 네크워크에 연결된 클라이언트 컴퓨터의 시스템이 바이러스에 대하여 어느 정도의 취약성을 갖는지를 제시해 주는 클라이언트 컴퓨터 분석 방법 및 그 시스템과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록매체에 관한 것이다.

일반적으로 컴퓨터 바이러스는 컴퓨터의 정상적인 동작에 영향을 미치거나 컴퓨터에 저장되어 있는 정보를 고의적으로 파괴하는 것과 같이 비정상적인 상태로 컴퓨터 시스템이 운용되도록 하는 프로그램이다. 즉, 바이러스에 감염된 프로그램으로 인하여 컴퓨터 시스템이 오동작하도록 하거나 보유한 데이터를 파괴 또는 컴퓨터 시스템 자체의 파괴를 일으키도록 한다.

반면, 컴퓨터를 사용하는 사용자들은 이러한 바이러스에 대한 지식을 거의 가지고 있지 못하여 자신의 컴퓨터가 어느 정도로 바이러스의 감염 위험에 노출되어 있는지 알지 못한다.

그러나, 이러한 위험에 대해서 분석, 리포트를 해주고 어드바이스(advice)를 제시해 주는 프로그램이 존재하지 않아 일반 사용자들은 바이러스에 대한 예방 대책을 세우기 어려웠다. 또한 모든 사용자가 각기 다른 환경에서 컴퓨터를 사용하고 있기 때문에 각 개인별 시스템, 사용하는 서비스 및 사용자 행위에 따라 각각 상황에 따른 개인별 분석이 필요하다.

발명이 이루고자하는 기술적 과제

본 발명은 상기 문제점을 해결하기 위하여 발명된 것으로서, 본 발명의 목적은 상기 일반 사용자들이 자신의 시스템이 바이러스에 얼마나 노출되어 있고 취약한 부분은 어느 부분인지 확인하고 조치할 수 있도록 하는 클라이언트 컴퓨터 분석 방법 및 그 시스템과 상기 방법을 실현시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록매체를 제공함을 그 목적으로 한다.

상기 목적을 달성하기 위한 본 발명은, 서버 및 통신 네트워크를 통해 상기 서버와 연결된 클라이언트 컴퓨터를 포함하는 클라이언트 컴퓨터 분석 시스템의 상기 클라이언트 컴퓨터에 대한 바이러스 취약성 정보를 제공하는 클라이언트 컴퓨터 분석 방법에 있어서, 상기 서버가 상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 제1단계, 상기 서버가 상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 제2단계, 상기 서버가 상기 제2단계에서 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 제3단계 및 상기 서버가 상기 제3단계에서 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의 브라우저로 전송하는 제4단계를 포함하되, 상기 시스템 분석 결과는 상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보를 포함하고, 상기 리포트는 하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고, 상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부를 포함함으로써 상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것을 특징으로 하는 클라이언트 컴퓨터 분석 방법을 제공한다.

또한, 상기 목적을 달성하기 위해 본 발명은, 통신 네트워크를 통해 클라이언트 컴퓨터와 연결된 클라이언트 컴퓨터 분석 시스템에 있어서, 상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 최신버전수단, 상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 수신수단, 상기 수신수단에 의해 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 리포트작성수단 및 상기 리포트작성수단에 의해 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의 브라우저로 전송하는 리포트전송수단을 포함하되, 상기 시스템 분석 결과는 상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보를 포함하고, 상기 리포트는 하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고, 상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부를 포함함으로써 상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것을 특징으로 하는 클라이언트 컴퓨터 분석 시스템을 제공한다.

또한, 상기 목적을 달성하기 위해 본 발명은, 클라이언트 컴퓨터에 대한 바이러스 취약성 정보를 제공하기 위해, 통신 네트워크를 통해 클라이언트 컴퓨터와 연결되며 프로세서를 포함한 클라이언트 컴퓨터 분석 시스템에, 상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 제1기능, 상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 제2기능, 상기 제2기능에 의해 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 제3기능 및 상기 제3기능에 의해 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의 브라우저로 전송하는 제4기능을 실현시키되, 상기 시스템 분석 결과는 상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보를 포함하고, 상기 리포트는 하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고, 상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부를 포함함으로써 상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한

다.

따라서 본 발명에 의하면, 종래의 패키지 형태의 프로그램이 아닌 온라인 프로그램으로서 인터넷이 가능한 곳에서는 별도의 복잡한 설치과정 없이 사용할 수 있으므로 프로그램을 휴대하고 다니거나 단일 컴퓨터에서만 사용하던 종래의 불편함을 해소하고, 어느 곳에서 컴퓨터를 사용하게 되더라도 위험성을 먼저 확인한 후에 사용할 수 있어 사전에 바이러스에 대한 위험을 제거하여 최근 급증하고 있는 바이러스에 대한 국가적인 차원의 손실을 예방할 수 있다.

본 발명이 속한 기술 분야에서 통상의 지식을 가진 자는 본 명세서의 도면, 발명의 상세한 설명 및 특허청구범위로부터 본 발명의 다른 목적 및 장점을 쉽게 인식할 수 있다.

발명의 구성 및 작용

이하의 내용은 단지 본 발명의 원리를 예시한다. 그러므로 당업자는 비록 본 명세서에 명확히 설명되거나 도시되지 않았지만 본 발명의 원리를 구현하고 본 발명의 개념과 범위에 포함된 다양한 장치를 발명할 수 있는 것이다. 또한, 본 명세서에 열거된 모든 조건부 용어 및 실시예들은 원칙적으로, 본 발명의 개념이 이해되도록 하기 위한 목적으로만 명백히 의도되고, 이와같이 특별히 열거된 실시예들 및 상태들에 제한적이지 않는 것으로 이해되어야 한다. 또한, 본 발명의 원리, 관점 및 실시예들 뿐만 아니라 특정 실시예를 열거하는 모든 상세한 설명은 이러한 사항의 구조적 및 기능적 균등물을 포함하도록 의도되는 것으로 이해되어야 한다. 또한 이러한 균등물들은 현재 공지된 균등물뿐만 아니라 장래에 개발될 균등물 즉 구조와 무관하게 동일한 기능을 수행하도록 발명된 모든 소자를 포함하는 것으로 이해되어야 한다.

프로세서 또는 이와 유사한 개념으로 표시된 기능 블럭을 포함하는 도면에 도시된 다양한 소자의 기능은 전용 하드웨어뿐만 아니라 적절한 소프트웨어와 관련하여 소프트웨어를 실행할 능력을 가진 하드웨어의 사용으로 제공될 수 있다. 프로세서에 의해 제공될 때, 상기 기능은 단일 전용 프로세서, 단일 공유 프로세서 또는 복수의 개별적 프로세서에 의해 제공될 수 있고, 이들 중 일부는 공유될 수 있다. 또한 프로세서, 제어가 또는 이와 유사한 개념으로 제시되는 용어의 명확한 사용은 소프트웨어를 실행할 능력을 가진 하드웨어를 배타적으로 인용하여 해석되어서는 아니되고, 제한 없이 디지털 신호 프로세서(DSP) 하드웨어, 소프트웨어를 저장하기 위한 롬(ROM), 램(RAM) 및 비 휘발성 메모리를 암시적으로 포함하는 것으로 이해되어야 한다. 주지관용의 다른 하드웨어도 포함될 수 있다. 특정의 기술은 본 명세서의 보다 상세한 이해로서 설계자에 의해 선택될 수 있다.

상술한 목적, 특징 및 장점들은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 우선 각 도면의 구성요소들에 참조 번호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 번호를 가지도록 하고 있음에 유의하여야 한다. 또한, 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명한다.

도1은 본 발명에 따른 서버에서의 작업진행을 도시한 순서도이다.

클라이언트 컴퓨터의 시스템이 바이러스에 어느 정도 취약한 지 여부를 분석하기 위하여 먼저, 서버는 클라이언트 컴퓨터에 어플리케이션 프로그램(Application Program)을 메시지 파일과 함께 제공한다(S10, S20). 상기 어플리케이션 프로그램으로는 액티브 엑스(Active X), 플러그 인(Plug In) 및 자바 애플릿(Java Applet) 등이 있다.

또한, 상기 메시지 파일은 사용자 동의창에 표시될 메시지를 저장한 파일로서, 상기 액티브 엑스, 플러그 인 및 자바 애플릿 등의 어플리케이션 프로그램은 로컬 시스템(local system)의 리소스(resource)를 직접 억세스(Access) 하기 때문에, 상기 다운로드 받을 시 인증 절차가 필요하다. 상기 인증 절차는 서버에서 클라이언트에게 상기 어플리케이션 프로그램에 대한 간략한 정보와 안정성 보장에 대한 정보를 담은 문서를 클라이언트 컴퓨터의 브라우저에 제공한다.

상기 클라이언트 컴퓨터의 시스템에 어플리케이션 프로그램이 존재하는 경우 또는 상기 어플리케이션 프로그램을 다운로드 받은 후에는 서버가 정보 파일을 상기 클라이언트 컴퓨터의 시스템에 다운로드 한다(S30).

상기 정보파일에는 상기 어플리케이션 프로그램에 포함된 파일들의 업데이트에 대한 정보가 저장되어 있는데, 예컨대, 상기 파일들의 사이즈, 생성 또는 갱신 날짜 및 설치 위치 등이 저장되어 있다.

상기 정보 파일을 클라이언트 컴퓨터로 다운로드 한 뒤, 상기 클라이언트 컴퓨터에서 처리된 분석결과를 공통 경로 인터페이스(CGI)를 이용하여 수신한다(S40).

상기 수신된 분석결과를 토대로 리포트를 작성하게 되는 데, 상기 리포트는 간단한 총평을 제공하며, 분석에 대한 세부 리포트는 시스템 영역, 응용프로그램 영역 및 안티바이러스 프로그램 영역으로 나누어 각각 작성된다(S50). 상기 리포트 작성 시에 필요한 문구는 미리 작성하여 서버에 저장되어 있으며, 필요에 따라 수정한다.

작성된 상기 리포트는 공통 경로 인터페이스(CGI)를 이용하여 상기 클라이언트 컴퓨터로 전송한다(S60).

도2는 본 발명에 따라 클라이언트 컴퓨터에서의 작업진행 과정을 도시한 순서도이다.

서버에 통신 네트워크로 연결된 클라이언트 컴퓨터의 익스플로러(Explorer) 또는 넷스케이프(Netscape) 중 하나에서 어플리케이션 프로그램(Application Program) 즉, 액티브 엑스, 플러그 인 또는 자바 애플릿 중 하나의 버전을 검사한다(S100).

상기 어플리케이션 프로그램에는 프로젝트 관련 파일, 액티브 엑스 관련 파일, 넷스케이프용 플러그 인

관련 파일 및 모듈 파일 등으로 구성되어 있다.

프로젝트 관련 파일은 상기 어플리케이션 프로그램의 버전을 통합관리하는 기능을 수행한다. 즉 프로젝트 관련 파일에 기초하여 어플리케이션 프로그램의 버전의 버전이 체크됨으로써 최신 버전이 유지될 수 있다.

모듈 파일에는 레지스트리 및 INI 파일 처리 모듈, 포트 스캔 관련 모듈, Http Post 관련 모듈, 시스템 정보 관련 모듈 등이 있다. 이러한 모듈 파일이 포함된 어플리케이션 프로그램이 클라이언트 컴퓨터에 다운로드되어 설치되면 후술되는 바와 같이 도3의 본 발명에 따른 클라이언트 컴퓨터로 구성된다. 예를 들어 레지스트리 및 INI 파일 처리 모듈, 포트 스캔 관련 모듈 및 시스템 정보 관련 모듈은 시스템 분석 모듈(250, 도3 참조)를 구성하게 되고, Http Post 관련 모듈은 분석 결과 전송 모듈(260, 도3 참조)를 구성하게 된다.

이미 어플리케이션 프로그램이 설치된 클라이언트 컴퓨터 시스템이 서버에 접속하게 될 경우 상기 어플리케이션 프로그램의 버전이 최신 버전이 아니라면 업데이트를 한다(S105, S107).

상기 어플리케이션 프로그램의 버전이 최신 버전인 경우, 서버로부터 상기 클라이언트 컴퓨터에 다운로드(S30)된 정보 파일에 있는 정보를 이용해 버전을 체크하게 된다(S110).

상기 정보 파일의 비교 결과 상기 클라이언트 컴퓨터에 저장되어 있는 상기 어플리케이션 프로그램에 포함된 파일들의 버전이 최신 버전이 아닌 경우에는 최신버전이 아닌 상기 파일들을 서버의 최신버전파일로 다운로드 하여 업데이트를 하며, 최신 버전인 경우에는 상기 클라이언트 컴퓨터의 시스템을 분석하게 된다(S115, S117, S120).

상기 어플리케이션 프로그램에 포함된 파일들의 일예로는 레지스트리 처리에 대한 명령을 저장한 파일, 포트 스캔에 사용되는 파일, 및 트로이 목마 바이러스 포트 리스트가 저장된 파일 등이 있다.

상기 클라이언트 컴퓨터의 시스템을 분석하는데 있어 크게 하드웨어와 소프트웨어로 나눈다. 그러나, 클라이언트에 따라 사용하는 하드웨어와 소프트웨어가 다양하므로 레지스트리(Resistry), INI 파일 및 포트 스캔(Port Scan)을 검색한다.

상기 레지스트리는 윈도우, 하드웨어, 소프트웨어 및 사용자에 관련된 모든 정보를 가지고 있는 두 파일 즉 System.dat과 User.dat을 통틀어서 가리키는 말이다.

보다 구체적으로 레지스트리는 6개의 서브트리로 구성되어 있는데, OLE(Object Linking and Embedding, 개체연결 및 삽입) 데이터 및 파일의 각 확장자에 대한 정보 및 각 파일과 프로그램간의 연결에 대한 정보를 포함하는 서브트리(HKEY_CLASSES_ROOT), 컴퓨터의 환경설정들에 대한 정보를 포함하는 서브트리(HKEY_CURRENT_USER), 컴퓨터에 설치된 하드웨어와 하드웨어를 구동시키는데 필요한 드라이버나 설정사항에 관련된 정보를 포함하는 서브트리(HKEY_LOCAL_MACHINE), 상기 HKEY_CURRENT_USER에 저장된 정보 전체와 데스크탑 설정, 네트워크 연결등의 정보를 포함하여 User.dat에 저장하는 서브트리(HKEY_USERS), 상기 HKEY_LOCAL_MACHINE의 서브트리로 존재하는 구성의 정보를 포함하는 서브트리(HKEY_CURRENT_CONFIG) 및 HKEY_DYN_DATA의 6개 서브트리이다.

즉 레지스트리의 항목들은 하드웨어, 소프트웨어, 유저 및 PC 또는 네트워크의 특성들을 나타내는 값들로 구성되어 있으며, 유저가 세팅을 하거나 새로운 소프트웨어를 설치하게 되면 레지스트리는 그 변화를 반영하여 바뀌게 된다.

상기 System.dat 파일에는 윈도우와 하드웨어 및 소프트웨어의 일부 정보를 가지고 있으며, User.dat 파일에는 소프트웨어 정보와 사용자에 관한 정보를 가지고 있다.

또한 INI 파일은 설정 파일로 클라이언트 컴퓨터의 오퍼레이팅 시스템인 윈도우의 자체 설정 파일인 System.ini와 Win.ini 파일이 있으며 이들은 상기 레지스트리와 관련되어 있으며, 레지스트리와 유사한 정보를 포함한다.

본 발명에 따르면 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램이 클라이언트 컴퓨터에 설치되어 레지스트리 및 INI 파일의 항목을 검사함으로써 클라이언트 컴퓨터에 설치되어 있는 소프트웨어 및 안티바이러스 소프트웨어의 설치여부 및 클라이언트 컴퓨터의 시스템 정보를 확인할 수 있으며, 이를 기초로 클라이언트 컴퓨터 시스템을 분석하여 소프트웨어 및 안티바이러스 소프트웨어의 설치여부, 클라이언트 컴퓨터의 시스템의 네트워크 구성요소, 공유 여부를 클라이언트 컴퓨터의 분석결과로서 서버로 전송하게 된다.

한편, 포트스캔이란 컴퓨터와 네트워크가 통신을 수행할 수 있는 통로 즉 포트가 열려있는지 여부를 확인하는 과정으로서, 본 발명에 따르면 면 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램이 클라이언트 컴퓨터에 설치되어 포트스캔에 의해 클라이언트 컴퓨터의 포트 열려있는지 여부를 확인할 수 있으며, 이를 기초로 클라이언트 컴퓨터 시스템을 분석하여 바이러스가 유입될 수 있는 포트가 열려 있는지를 클라이언트 컴퓨터의 분석결과로서 서버로 전송하게 된다. 포트스캔은 이미 공지되어 있는 기술이므로, 그 상세한 설명은 생략한다.

상기 분석 항목들을 수집한 결과 즉 소프트웨어 및 안티바이러스 소프트웨어의 설치여부, 클라이언트 컴퓨터의 시스템의 네트워크 구성요소, 공유 여부 및 바이러스가 유입될 수 있는 포트가 열려 있는지 여부를 포스트(post)방식을 사용하여 서버측 공통 경로 인터페이스(CGI)로 전송한다(S130).

전송된 데이터를 이용해서 서버에서는 클라이언트 컴퓨터 시스템의 취약성을 분석하고, 상기 분석결과를 기초로 하여 서버에서 작성된 리포트를 상기 클라이언트 컴퓨터에서 수신하여 파일로 저장을 한다(S140, S150).

예를 들어, 클라이언트 컴퓨터에 설치되어 있는 소프트웨어 존재 여부의 분석결과를 기초로 "설치해서 사용하고 계시는 프로그램 중에 바이러스에 취약한 프로그램이 있습니다."와 같이 클라이언트 컴퓨터에

설치된 소프트웨어가 바이러스에 감염될 수 있다는 정보를 응용 프로그램 영역의 리포트로서 제공하고, 클라이언트 컴퓨터에 설치되어 있는 안티바이러스 소프트웨어 존재 여부의 분석결과를 기초로 "안티바이러스 프로그램을 사용하고 있으며 이 프로그램을 주기적으로 업데이트 해 주시고 항상 시스템 감시를 실행시켜 두시면 안전합니다."와 같이 클라이언트 컴퓨터에 설치된 안티바이러스 소프트웨어에 의해 바이러스 감염의 위험으로부터 어느 정도 안심할 수 있다는 정보를 안티바이러스 프로그램 영역의 리포트로서 제공하며, 클라이언트 컴퓨터의 네트워크 설정 여부의 분석결과를 기초로 "시스템에 CD-ROM이 장착되어 있습니다. 만약 바이러스가 포함되어 있는 CD를 사용하실 경우 바이러스에 감염될 가능성이 있습니다."와 같이 클라이언트 컴퓨터의 네트워크 설정 상황에 따라 클라이언트 컴퓨터가 바이러스에 감염될 수 있다는 정보를 하드웨어 영역의 리포트로서 제공하며, 바이러스가 유입될 수 있는 포트가 열려 있는지 여부의 분석결과를 기초로 "현재 시스템에는 트로이 목마가 사용하는 Listen Port가 있습니다. 그러나 반드시 트로이 목마가 감염되어 있는 것은 아니니 최신 엔진으로 업데이트된 백신 프로그램이나 진단 프로그램을 통해 검사하셔서 이상이 없으면 안심해도 됩니다."와 같이 포트가 열려있는지 여부에 따라 바이러스에 감염될 수 있다는 정보를 하드웨어 영역의 리포트로서 제공하게 된다.

상기와 같은 각 영역의 리포트를 취합하여, "인터넷에 연결할 수 있는 상태이며 인터넷을 통해 바이러스가 유입될 수 있으며 트로이 목마를 통한 해킹의 위험도 있습니다."와 같이 클라이언트 시스템에 대한 전반적인 정보를 총평의 리포트로서 제공하게 된다.

즉, 이상에서 살펴본 바와 같이 본 발명에 따라 클라이언트 컴퓨터로부터 제공되는 분석결과는 레지스트리, INI 파일 및 포트스캔으로부터 확인할 수 있는 소프트웨어 존재 여부, 클라이언트 컴퓨터의 네트워크 설정 여부 등이고, 상기 분석결과를 기초로 서버가 수행하는 클라이언트 컴퓨터의 취약성 분석 및 리포트는 상기 분석결과 즉 소프트웨어의 존재 여부, 클라이언트 컴퓨터의 네트워크 설정 여부로부터 파악할 수 있는 바이러스 감염 가능성 여부이다. 따라서, 서버가 미리 작성되어 있는 문구들을 조합하여 각 영역의 리포트를 작성하는 것이 가능하다.

상기 저장된 파일을 상기 클라이언트 컴퓨터의 브라우저로 경로를 재 지정하여 상기 결과 값을 상기 브라우저에 출력하도록 한다(S160).

도3은 본 발명에 따른 서버와 클라이언트 컴퓨터의 구성도로서, 작동순서에 따라 설명한다.

서버(100)는 HTTP 데몬(110), 최신버전모듈(120), 데이터베이스(130) 및 공통 경로 인터페이스(CGI) 모듈(140)을 포함하여 구성되어 있으며, 상기 공통 경로 인터페이스(CGI) 모듈(140)에는 수신모듈(141), 리포트 작성모듈(143), 및 리포트 전송모듈(145)로 구성되어 있다.

클라이언트 컴퓨터(200)는 웹브라우저(210), 업데이트 모듈(220), 버전관리모듈(230), 분석항목 업데이트 모듈(240), 시스템 분석 모듈(250), 분석결과 전송모듈(260), 리포트 수신모듈(270), 및 저장 및 경로 재지정 모듈(280)을 포함하여 구성되어 있다.

또한, 상기 서버(100)와 통신 네트워크로 연결될 클라이언트 컴퓨터(200)는 하나 이상이며, 상기 통신 네트워크로는 인트라넷(intranet) 및 인터넷(internet) 등이 있다.

먼저, 통신 네트워크를 이용하여 클라이언트 컴퓨터(200)는 웹브라우저(210) 및 HTTP(HyperText Transfer Protocol) 데몬(110)을 통해 서버(100)로 접속한다.

상기 서버(100)에서는 액티브 엑스, 플러그 인 및 자바 애플릿 같은 어플리케이션 프로그램의 최신 버전 및 업데이트된 정보 파일을 보유, 갱신 및 상기 클라이언트 컴퓨터(200)에 다운로드 할 수 있는 최신버전모듈(120)이 있다.

클라이언트 컴퓨터(200)에는 상기 최신버전모듈(120)로부터 상기 최신 버전으로 업데이트된 정보 파일을 다운로드 받는 업데이트모듈(220)과, 다운로드 된 정보 파일을 최신 버전으로 유지 할 수 있도록 관리하는 버전관리모듈(230)이 있다.

상기 버전관리모듈(230)에서는 상기 서버(100)에서 다운로드 받은 정보 파일에 저장되어 있는 업데이트 대상 파일들의 정보 즉, 파일 생성 및 갱신 날짜, 파일들의 크기, 및 파일 설치 위치 등을 체크하여 업데이트할 파일이 있는지를 확인한다.

그리고, 상기 클라이언트 컴퓨터(200) 내의 분석 항목 업데이트 모듈(240)에서는 상기 체크된 업데이트 대상 파일을 다운로드하고 무결성을 검사한후 업데이트를 수행한다.

상기 업데이트 과정이 끝나면, 시스템 분석 모듈(250)이 클라이언트 컴퓨터에 대한 분석을 실시한다. 상기 시스템 분석 모듈(250)은 시스템 정보 처리 모듈, 레지스트리 처리모듈 및 외부 모듈을 연결하는 모듈로 구성되어 있다.

상기된 바와 같이, 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램의 레지스트리 및 INI 파일 처리 모듈은 레지스트리 처리 모듈을 구성하고, 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램의 포트 스캔 관련 모듈은 외부 모듈을 연결하는 모듈을 구성하며, 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램의 시스템 정보 관련 모듈은 시스템 정보 처리 모듈을 구성하게 된다.

상기 시스템 정보 처리 모듈은 운영 체제(OS), 네트워크 구성요소, 공유 등 시스템에 의존적인 내용들을 분석하여 처리하는 모듈이다.

상기 시스템 정보 처리 모듈은 운영 체제의 버전에 따라 윈95/98 시스템, 윈NT 4 서버/워크 및 윈2000프로로 나뉘어 분석하는 모듈이 따로 존재한다. 또한, 네트워크 구성요소 및 공유 등에 관한 분석항목으로는 모뎀 설치 여부, 랜카드 설치 여부, TCP/IP 설치 여부, IPX/SPX 설치 여부, 네트워크 파일 공유 서비스 설치 여부, 스크립트 호스트 설치 여부, CD-ROM 설치 여부, 외장형 드라이브의 존재 여부, 네트워크 연결 드라이브의 존재 여부, 인터넷 익스플로러 버전 정보, 공유 디렉토리 존재 여부, 발견된 트로이 목마 바이러스 포트 등이 있다.

그리고, 상기 시스템 분석 모듈(250)에 존재하는 레지스트리 처리 모듈은 레지스트리 및 INI 파일과 관련된 내용을 분석하는 모듈로 상기 분석항목 업데이트모듈(240)에서 얻어진 내용에 대한 검색을 처리한다.

이와같이, 본 발명에 따르면 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램이 클라이언트 컴퓨터에 설치되어 레지스트리 및 INI 파일의 항목을 검사함으로써 클라이언트 컴퓨터의 시스템 정보를 확인할 수 있으며, 이를 기초로 클라이언트 컴퓨터 시스템을 분석하게 된다.

마지막으로, 상기 시스템 분석 모듈(250)에는 외부 모듈과 연결하는 모듈이 존재하는데, 이는 제공된 포트 스캔의 다이나믹 링크 라이브러리(Dynamic Link Library, DLL)를 임포트(Import)하여 상기 포트 스캔을 지원한다.

이와같이, 본 발명에 따르면 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램이 클라이언트 컴퓨터에 설치되어 포트스캔을 수행함으로써 클라이언트 컴퓨터의 포트 정보를 확인할 수 있으며, 이를 기초로 클라이언트 컴퓨터 시스템을 분석하게 된다.

한편, 상기된 바와 같이 본 발명에 따르면 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램이 클라이언트 컴퓨터에 설치되어 레지스트리 및 INI 파일의 항목을 검사함으로써 클라이언트 컴퓨터에 설치되어 있는 소프트웨어 및 안티바이러스 소프트웨어의 설치여부를 확인할 수 있으며, 이를 기초로 클라이언트 컴퓨터 시스템을 분석하게 된다.

상기 시스템 분석 모듈(250)에서 얻은 분석 결과를 분석결과 전송모듈(260)에서 http 프로토콜의 포스트(post)형태로 클라이언트 컴퓨터(200)에서 서버(100)로 송신한다. 상기된 바와 같이 클라이언트 컴퓨터로 다운로드된 어플리케이션 프로그램의 Http Post 관련 모듈은 분석 결과 전송 모듈(260)을 구성하게 된다.

상기 서버(100)의 공통 경로 인터페이스 (CGI, Common Gateway Interface)모듈(140)의 수신모듈(141)에서 상기 분석결과를 수신하여, 상기 서버의 리포트 작성모듈(143)에서 리포트를 작성한다.

상기 리포트는 상기된 바와 같이 미리 작성되어 있는 문구들을 조합하여 상기 분석결과에 기초하여 총평을 작성하고 자세한 결과를 하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 나뉘어 각각 작성하게 된다.

상기 리포트를 작성한 후, 상기 서버(100)의 리포트 전송모듈(145)를 통해 클라이언트 컴퓨터(200)의 리포트 수신모듈(270)로 전송한다.

상기 수신된 리포트는 저장 및 경로 재지정 모듈(280)에서 상기 클라이언트 컴퓨터(200)에 파일로 저장되고, 또한 경로가 상기 클라이언트 컴퓨터(200)의 웹브라우저(210)로 재지정되어 출력된다.

상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록매체(시디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다.

이상에서 설명한 본 발명은 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니고, 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하다는 것이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어서 명백하다 할 것이다.

발명의 효과

이상에서 상세히 설명한 바와 같이, 본 발명의 온라인 바이러스 취약성 분석도구에 의하면, 종래의 패키지 형태의 프로그램이 아닌 온라인 프로그램으로서 인터넷이 가능한 곳에서는 별도의 복잡한 설치과정 없이 사용할 수 있으므로 프로그램을 휴대하고 다니거나 단일 컴퓨터에서만 사용하던 종래의 불편함을 해소하고, 어느 곳에서 컴퓨터를 사용하게 되더라도 위험성을 먼저 확인한 후에 사용할 수 있어 사전에 바이러스에 대한 위험을 제거하여 최근 급증하고 있는 바이러스에 대한 국가적인 차원의 손실을 예방할 수 있다.

또한, 기존의 온라인 서비스를 이용해서 제공되는 바이러스 진단 및 치료 프로그램인 MyV3와 함께 연계하여 이용하면 감염된 바이러스를 온라인 상에서 진단 및 치료 할 수 있을 뿐만 아니라 그 전에 바이러스 취약점을 분석하여 미리 예방조치를 취하여 바이러스에 대한 피해를 더욱 효과적으로 막아낼 수 있다.

(57) 청구의 범위

청구항 1

서버 및 통신 네트워크를 통해 상기 서버와 연결된 클라이언트 컴퓨터를 포함하는 클라이언트 컴퓨터 분석 시스템의 상기 클라이언트 컴퓨터에 대한 바이러스 취약성 정보를 제공하는 클라이언트 컴퓨터 분석 방법에 있어서,

상기 서버가 상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 제1단계;

상기 서버가 상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 제2단계;

상기 서버가 상기 제2단계에서 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 제3단계; 및

상기 서버가 상기 제3단계에서 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의

브라우저로 전송하는 제4단계

를 포함하되,

상기 시스템 분석 결과는

상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보

를 포함하고,

상기 리포트는

하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고,

상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부

를 포함함으로써

상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 2

제1항에 있어서,

상기 어플리케이션 프로그램은

적어도 상기 클라이언트 컴퓨터의 시스템 분석 항목인 레지스트리 정보, INI 파일 정보 및 포트스캔 정보 중 어느 하나

를 포함하고,

상기 정보 파일은

상기 레지스트리 정보, INI 파일 정보 및 포트스캔 정보의 생성 및 업데이트 일자, 사이즈 및 설치 위치 등에 대한 업데이트 정보

를 포함하는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 3

제1항 또는 제2항에 있어서,

상기 제1단계는

상기 클라이언트 컴퓨터 시스템에 상기 어플리케이션 프로그램이 이미 설치되어 있는지 여부를 확인하는 제5단계;

상기 제5단계의 확인 결과 상기 어플리케이션 프로그램이 설치되어 있지 않은 경우에는 상기 어플리케이션 프로그램을 상기 클라이언트 컴퓨터로 다운로드시키는 제6단계;

상기 제5단계의 확인 결과 상기 어플리케이션 프로그램이 이미 설치되어 있는 경우에는 상기 어플리케이션 프로그램이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 어플리케이션 프로그램을 최신 버전으로 업데이트 시키는 제7단계; 및

상기 정보 파일이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 정포 파일을 최신 버전으로 업데이트 시키는 제8단계

를 포함하는 클라이언트 컴퓨터 분석 방법.

청구항 4

제1항 또는 제2항에 있어서,

상기 어플리케이션 프로그램은

상기 정보 파일을 다운로드 받기 위한 업데이트 모듈;

상기 다운로드된 정보 파일에 저장되어 있는 업데이트 정보를 기초로 업데이트할 파일이 존재하는지 여부를 확인하는 버전관리모듈;

상기 버전관리모듈의 확인 결과 업데이트할 파일이 존재하는 경우 당해 업데이트할 파일을 상기 서버로부터 다운로드받고, 상기 다운로드 받은 파일의 무결성을 검증하며, 상기 무결성이 검증된 파일을 상기 클라이언트 컴퓨터에 설치함으로써 상기 클라이언트 컴퓨터에 대해 분석할 시스템 분석 항목을 업데이트 시키는 분석항목업데이트모듈;

상기 업데이트된 시스템 분석 항목에 따라 상기 클라이언트 컴퓨터의 레지스트리 및 INI 파일의 항목을 검사하고 포트스캔을 수행함으로써 상기 클라이언트 컴퓨터에 설치되어 있는 응용 프로그램 및 안티바이러스 프로그램의 설치여부 및 클라이언트 컴퓨터의 시스템 정보를 포함하는 상기 클라이언트 컴퓨터의 시스템을 분석하는 시스템분석모듈; 및

상기 시스템분석모듈의 시스템 분석 결과를 하이퍼텍스트 프로토콜(http)의 포스트(post) 형태로 상기 서버로 전송하는 분석결과전송모듈; 및

상기 서버로부터 수신된 상기 리포트를 상기 클라이언트 컴퓨터에 파일로 저장하고, 상기 파일의 경로를 상기 클라이언트 컴퓨터의 브라우저로 재지정하여 상기 리포트를 출력하는 저장및경로재지정모듈

을 포함하는 것을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 5

제4항에 있어서,

상기 어플리케이션 프로그램은

액티브 엑스, 플러그 인 및 자바 애플릿 중 어느 하나인 것

을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 6

제1항에 있어서,

상기 리포트는

하이퍼텍스트 마크업 언어(HTML)로 작성되는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 7

제1항에 있어서,

상기 클라이언트 컴퓨터는

적어도 하나 이상인 것

을 특징으로 하는 클라이언트 컴퓨터 분석 방법.

청구항 8

통신 네트워크를 통해 클라이언트 컴퓨터와 연결된 클라이언트 컴퓨터 분석 시스템에 있어서,

상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 최신버전수단;

상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 수신수단;

상기 수신수단에 의해 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 리포트작성수단; 및

상기 리포트작성수단에 의해 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의 브라우저로 전송하는 리포트전송수단

을 포함하되,

상기 시스템 분석 결과는

상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보

를 포함하고,

상기 리포트는

하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고,

상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부

를 포함함으로써

상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 9

제8항에 있어서,

상기 어플리케이션 프로그램은

적어도 상기 클라이언트 컴퓨터의 시스템 분석 항목인 레지스트리 정보, INI 파일 정보 및 포트스캔 정보 중 어느 하나

를 포함하고,

상기 정보 파일은

상기 레지스트리 정보, INI 파일 정보 및 포트스캔 정보의 생성 및 업데이트 일자, 사이즈 및 설치 위치 등에 대한 업데이트 정보

를 포함하는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 10

제8항 또는 제9항에 있어서,

상기 최신버전수단은

상기 클라이언트 컴퓨터 시스템에 상기 어플리케이션 프로그램이 이미 설치되어 있는지 여부를 확인하고,

상기 어플리케이션이 이미 설치되어 있는지 여부의 확인 결과 상기 어플리케이션 프로그램이 설치되어 있지 않은 경우에는 상기 어플리케이션 프로그램을 상기 클라이언트 컴퓨터로 다운로드시키고,

상기 어플리케이션이 이미 설치되어 있는지 여부의 확인 결과 상기 어플리케이션 프로그램이 이미 설치되어 있는 경우에는 상기 어플리케이션 프로그램이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 어플리케이션 프로그램을 최신 버전으로 업데이트 시키며,

상기 정보 파일이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 정포 파일을 최신 버전으로 업데이트 시키는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 11

제8항 또는 제9항에 있어서,

상기 어플리케이션 프로그램은

상기 정보 파일을 다운로드 받기 위한 업데이트 모듈;

상기 다운로드된 정보 파일에 저장되어 있는 업데이트 정보를 기초로 업데이트할 파일이 존재하는지 여부를 확인하는 버전관리모듈;

상기 버전관리모듈의 확인 결과 업데이트할 파일이 존재하는 경우 당해 업데이트할 파일을 상기 서버로부터 다운로드받고, 상기 다운로드 받은 파일의 무결성을 검증하며, 상기 무결성이 검증된 파일을 상기 클라이언트 컴퓨터에 설치함으로써 상기 클라이언트 컴퓨터에 대해 분석할 시스템 분석 항목을 업데이트 시키는 분석항목업데이트모듈;

상기 업데이트된 시스템 분석 항목에 따라 상기 클라이언트 컴퓨터의 레지스트리 및 INI 파일의 항목을 검사하고 포트스캔을 수행함으로써 상기 클라이언트 컴퓨터에 설치되어 있는 응용 프로그램 및 안티바이러스 프로그램의 설치여부 및 클라이언트 컴퓨터의 시스템 정보를 포함하는 상기 클라이언트 컴퓨터의 시스템을 분석하는 시스템분석모듈; 및

상기 시스템분석모듈의 시스템 분석 결과를 하이퍼텍스트 프로토콜(http)의 포스트(post) 형태로 상기 서버로 전송하는 분석결과전송모듈; 및

상기 서버로부터 수신된 상기 리포트를 상기 클라이언트 컴퓨터에 파일로 저장하고, 상기 파일의 경로를 상기 클라이언트 컴퓨터의 브라우저로 재지정하여 상기 리포트를 출력하는 저장및경로재지정모듈

을 포함하는 것을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 12

제11항에 있어서,

상기 어플리케이션 프로그램은

액티브 엑스, 플러그 인 및 자바 애플릿 중 어느 하나인 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 13

제8항에 있어서,

상기 리포트는

하이퍼텍스트 마크업 언어(HTML)로 작성되는 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 14

제8항에 있어서,

상기 클라이언트 컴퓨터는

적어도 하나 이상인 것

을 특징으로 하는 클라이언트 컴퓨터 분석 시스템.

청구항 15

클라이언트 컴퓨터에 대한 바이러스 취약성 정보를 제공하기 위해, 통신 네트워크를 통해 클라이언트 컴퓨터와 연결되며 프로세서를 포함한 클라이언트 컴퓨터 분석 시스템에,

상기 클라이언트 컴퓨터의 시스템을 분석하기 위한 어플리케이션 프로그램 및 상기 어플리케이션 프로그램이 이용하는 정보 파일을 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터로 제공하는 제1기능;

상기 어플리케이션 프로그램에 의한 상기 클라이언트 컴퓨터의 시스템 분석 결과를 상기 통신 네트워크를 통해 수신하는 제2기능;

상기 제2기능에 의해 수신한 상기 시스템 분석 결과를 기초로 리포트를 작성하는 제3기능; 및

상기 제3기능에 의해 작성된 리포트를 상기 통신 네트워크를 통해 상기 클라이언트 컴퓨터의 브라우저로 전송하는 제4기능

을 실현시키되,

상기 시스템 분석 결과는

상기 클라이언트 컴퓨터에 설정되어 있는 레지스트리 및 INI 파일 검색 및 상기 클라이언트 컴퓨터에 대한 포트스캔으로부터 확인할 수 있는 응용 프로그램 존재 여부 정보, 안티바이러스 프로그램 존재 여부 정보 및 상기 클라이언트 컴퓨터의 네트워크 설정 여부 정보

를 포함하고,

상기 리포트는

하드웨어 영역, 응용 프로그램 영역 및 안티바이러스 프로그램 영역으로 각각 작성되고,

상기 시스템 분석 결과로부터 파악할 수 있는 바이러스 감염 가능성 여부

를 포함함으로써

상기 클라이언트 컴퓨터 시스템의 바이러스 취약성에 대해 리포트를 하는 것

을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 16

제15항에 있어서,

상기 어플리케이션 프로그램은

적어도 상기 클라이언트 컴퓨터의 시스템 분석 항목인 레지스트리 정보, INI 파일 정보 및 포트스캔 정보 중 어느 하나

를 포함하고,

상기 정보 파일은

상기 레지스트리 정보, INI 파일 정보 및 포트스캔 정보의 생성 및 업데이트 일자, 사이즈 및 설치 위치 등에 대한 업데이트 정보

를 포함하는 것

을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 17

제15항 또는 제16항에 있어서,

상기 제1기능은

상기 클라이언트 컴퓨터 시스템에 상기 어플리케이션 프로그램이 이미 설치되어 있는지 여부를 확인하는 제5기능;

상기 제5기능의 확인 결과 상기 어플리케이션 프로그램이 설치되어 있지 않은 경우에는 상기 어플리케이션 프로그램을 상기 클라이언트 컴퓨터로 다운로드시키는 제6기능;

상기 제5기능의 확인 결과 상기 어플리케이션 프로그램이 이미 설치되어 있는 경우에는 상기 어플리케이션 프로그램이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 어플리케이션 프로그램을 최신 버전으로 업데이트 시키는 제7기능; 및

상기 정보 파일이 최신 버전인지 여부를 확인하여 최신 버전이 아닌 경우에는 상기 정포 파일을 최신 버전으로 업데이트 시키는 제8기능

을 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 18

제15항 또는 제16항에 있어서,

상기 어플리케이션 프로그램은

상기 정보 파일을 다운로드 받기 위한 업데이트 모듈;

상기 다운로드된 정보 파일에 저장되어 있는 업데이트 정보를 기초로 업데이트할 파일이 존재하는지 여부를 확인하는 버전관리모듈;

상기 버전관리모듈의 확인 결과 업데이트할 파일이 존재하는 경우 당해 업데이트할 파일을 상기 서버로부터 다운로드받고, 상기 다운로드 받은 파일의 무결성을 검증하며, 상기 무결성이 검증된 파일을 상기 클라이언트 컴퓨터에 설치함으로써 상기 클라이언트 컴퓨터에 대해 분석할 시스템 분석 항목을 업데이트시키는 분석항목업데이트모듈;

상기 업데이트된 시스템 분석 항목에 따라 상기 클라이언트 컴퓨터의 레지스트리 및 INI 파일의 항목을 검사하고 포트스캔을 수행함으로써 상기 클라이언트 컴퓨터에 설치되어 있는 응용 프로그램 및 안티바이러스 프로그램의 설치여부 및 클라이언트 컴퓨터의 시스템 정보를 포함하는 상기 클라이언트 컴퓨터의 시스템을 분석하는 시스템분석모듈; 및

상기 시스템분석모듈의 시스템 분석 결과를 하이퍼텍스트 프로토콜(http)의 포스트(post) 형태로 상기 서버로 전송하는 분석결과전송모듈; 및

상기 서버로부터 수신된 상기 리포트를 상기 클라이언트 컴퓨터에 파일로 저장하고, 상기 파일의 경로를 상기 클라이언트 컴퓨터의 브라우저로 재지정하여 상기 리포트를 출력하는 저장및경로재지정모듈

을 포함하는 것을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 19

제18항에 있어서,

상기 어플리케이션 프로그램은

액티브 엑스, 플러그 인 및 자바 애플릿 중 어느 하나인 것

을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 20

제15항에 있어서,

상기 리포트는

하이퍼텍스트 마크업 언어(HTML)로 작성되는 것

을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 21

제15항에 있어서,

상기 클라이언트 컴퓨터는

적어도 하나 이상인 것

을 특징으로 하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 22

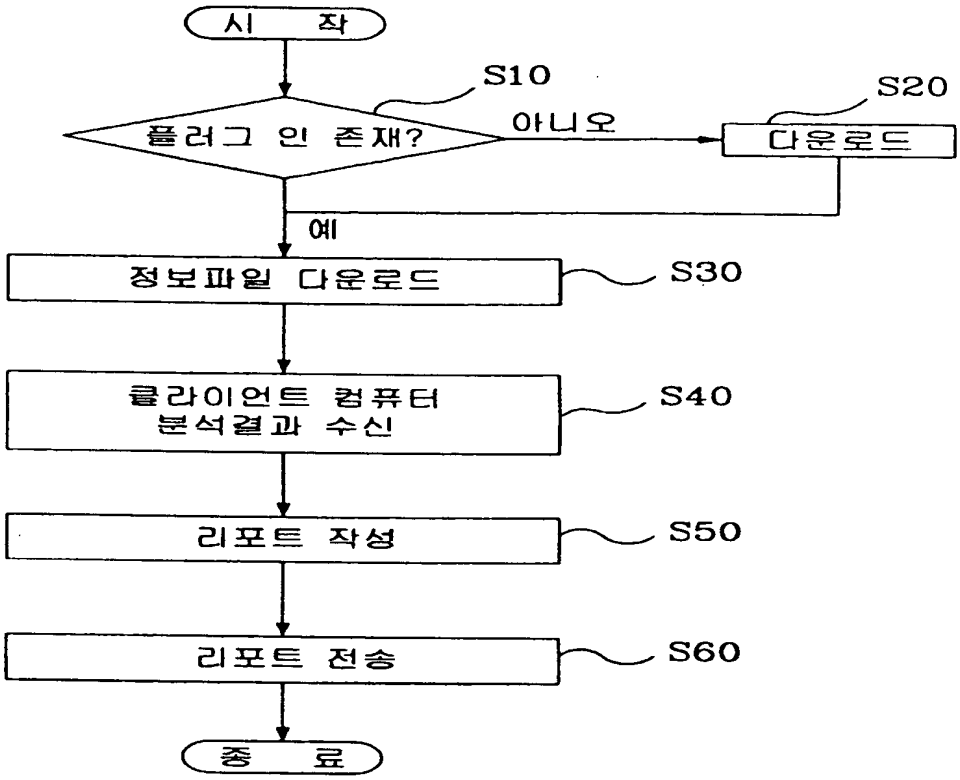
삭제

청구항 23

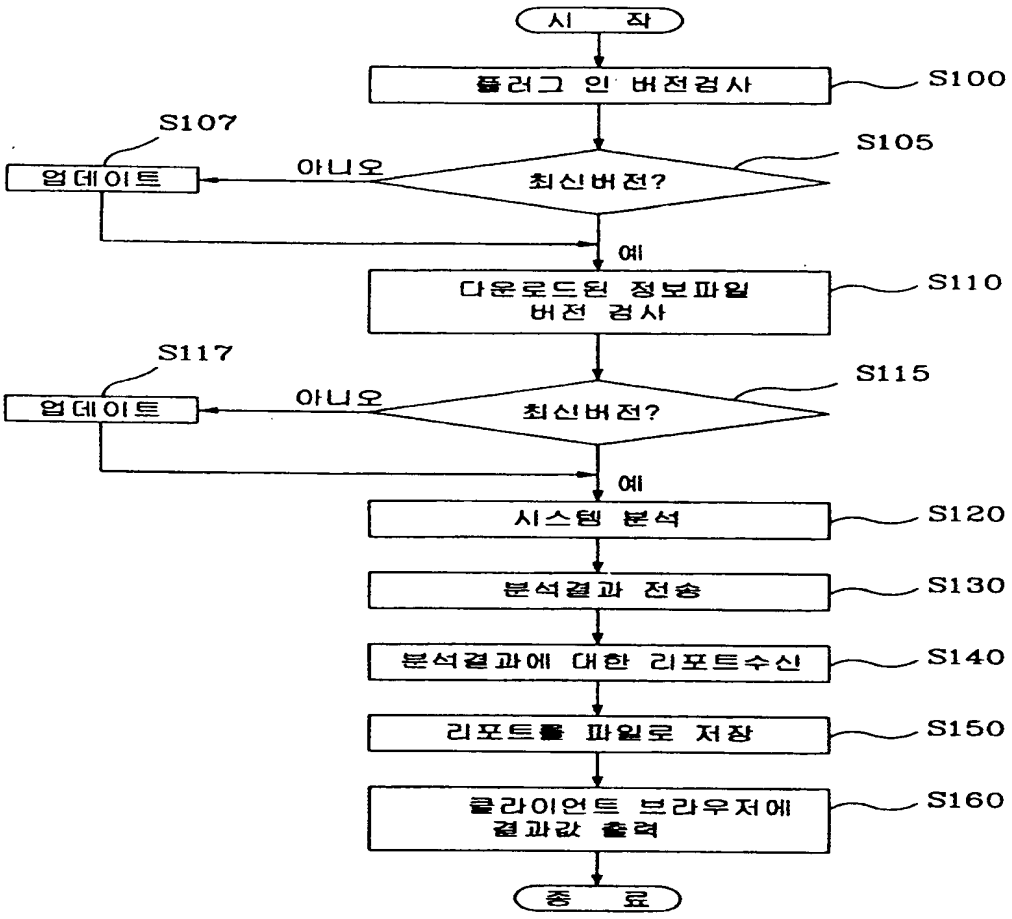
삭제

도면

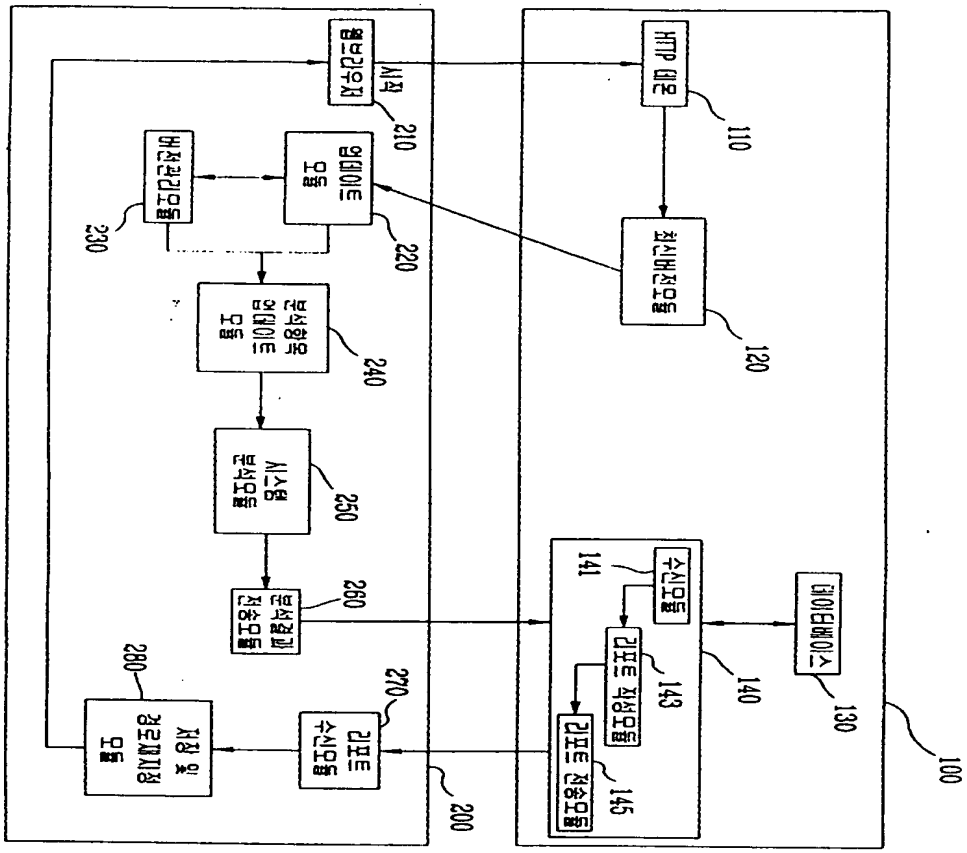
도면1


시 작
S10
플러그 인 존재?
아니오
S20
다운로드
예
정보파일 다운로드
S30
클라이언트 컴퓨터
분석결과 수신
S40
리포트 작성
S50
리포트 전송
S60
종 료

도면2


시 작
플러그 인 버전검사
S100
S105
최신버전?
아니오
S107
업데이트
예
다운로드된 정보파일 버전 검사
S110
S115
최신버전?
아니오
S117
업데이트
예
시스템 분석
S120
분석결과 전송
S130
분석결과에 대한 리포트수신
S140
리포트를 파일로 저장
S150
클라이언트 브라우저에 결과값 출력
S160
종 료

도면3


HTTP 데몬
110
최신버전모듈
120
데이터베이스
130
140
수신모듈
141
리포트 작성모듈
143
리포트 전송모듈
145
100
시작
210
업데이트 모듈
220
버전관리모듈
230
업데이트 설정 모듈
240
시스템 설정모듈
250
업데이트 전송모듈
260
리포트 수신모듈
270
자동 및 수동 체크모듈
280
200